나무위키

GNUnet

최근 수정 시각: 2026-08-23 05:36:29

분류:프록시 | 파일 공유 | 다크 웹 | GNU

GNU Project
[펼치기 · 접기]

목차

1. 개요
2. 설치 방법
3. 한계
4. 억압적인 국가에서의 검열 우회

https://www.gnunet.org/en/

1. 개요

GNUnet이란 안전하고 분산적이며 개인 정보를 보호하는 애플리케이션을 구축하기 위한 네트워크 프로토콜 스택이다.

GNUnet의 개념이 추상적이고 관련 정보를 찾기 어려워서 GNUnet을 이해하기란 쉽지 않다.

GNUnet의 여러 기능 중에서 가장 많이 알려진 기능은 파일 공유이다.

GNUnet에 대해서 다음의 글들을 참고할 수 있다.참고글1@,참고글2@,참고글3@,참고글4@,참고글5@

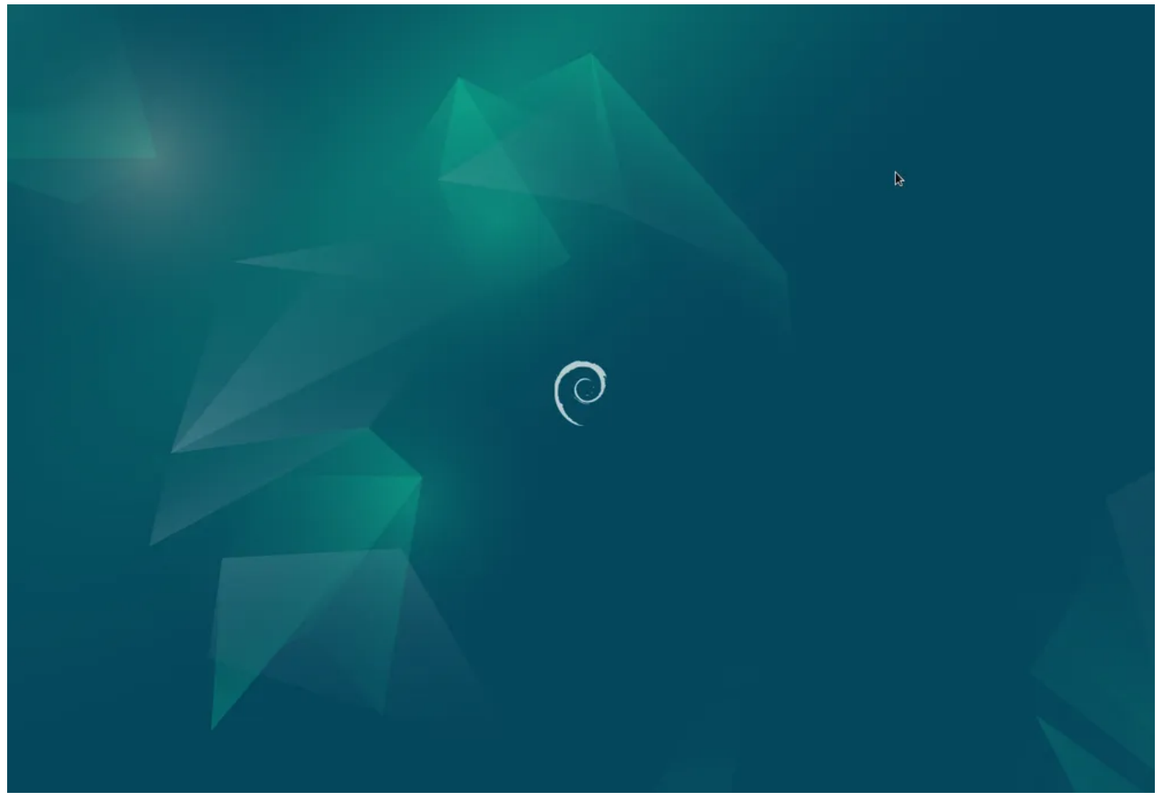
2. 설치 방법

참고사항
1. GNUnet은 윈도우에서 사용할 수 없다. 따라서 GNUnet을 사용하려면 무조건 리눅스를 설치해야 한다.
2. GNUnet은 이용자가 거의 없어서 파일을 검색해도 아무것도 나오지 않을 수 있다.

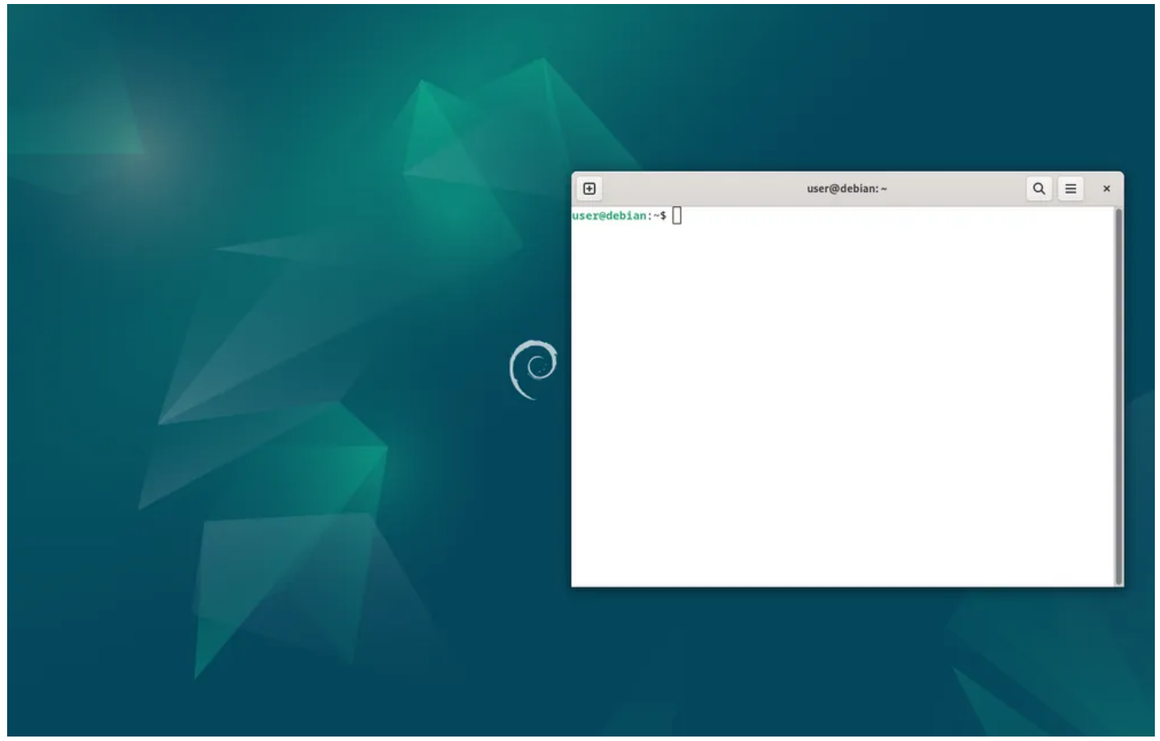
GNUnet 설치하는 법

데비안에서 GNUnet을 설치하고 이용하는 방법을 알아보자.

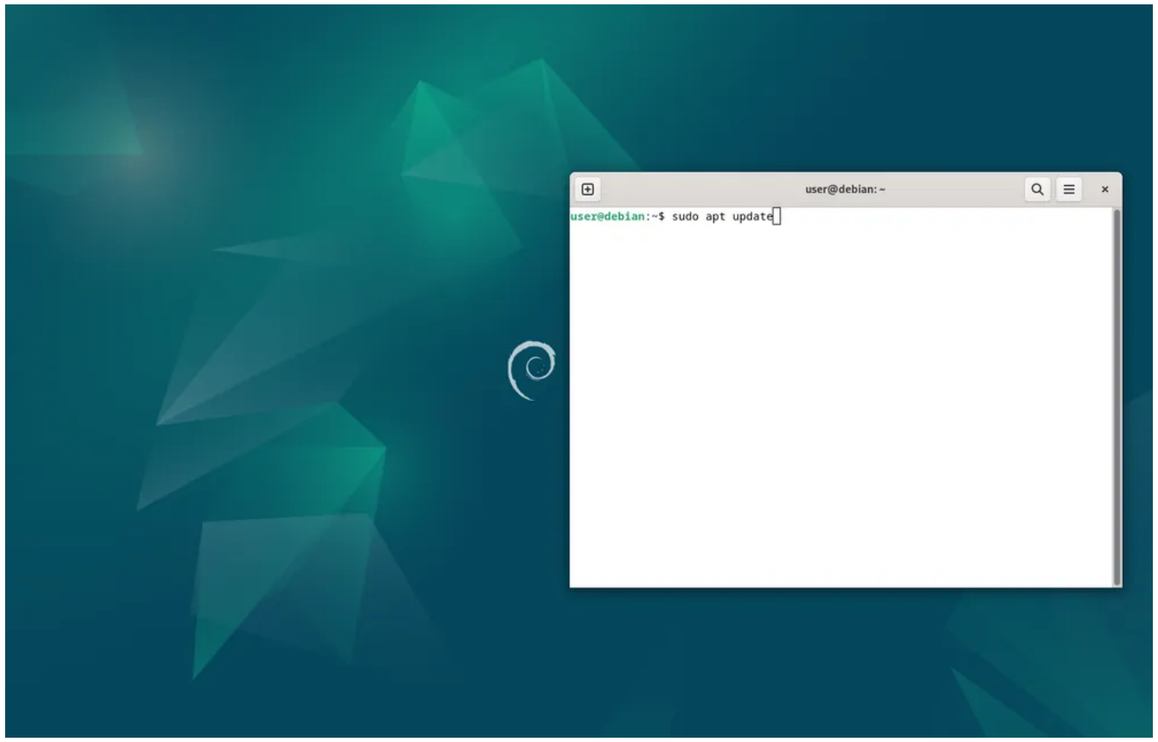
1. 데비안을 켠다.

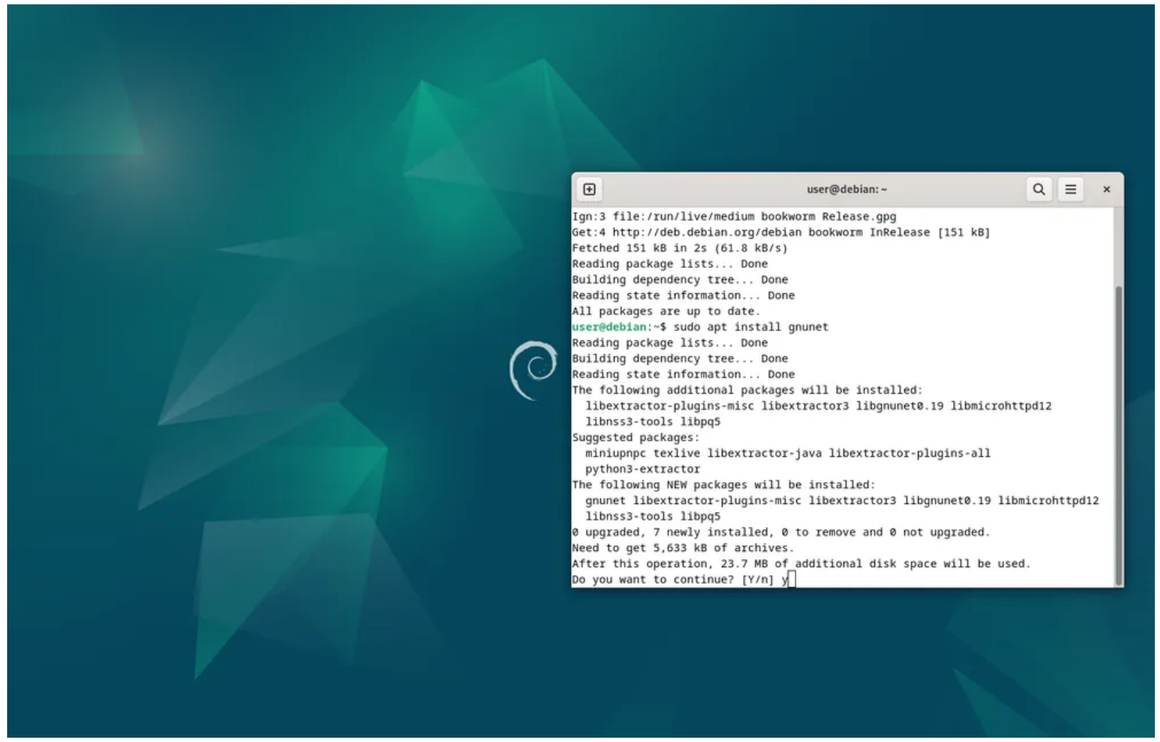


2. 터미널을 켠다.

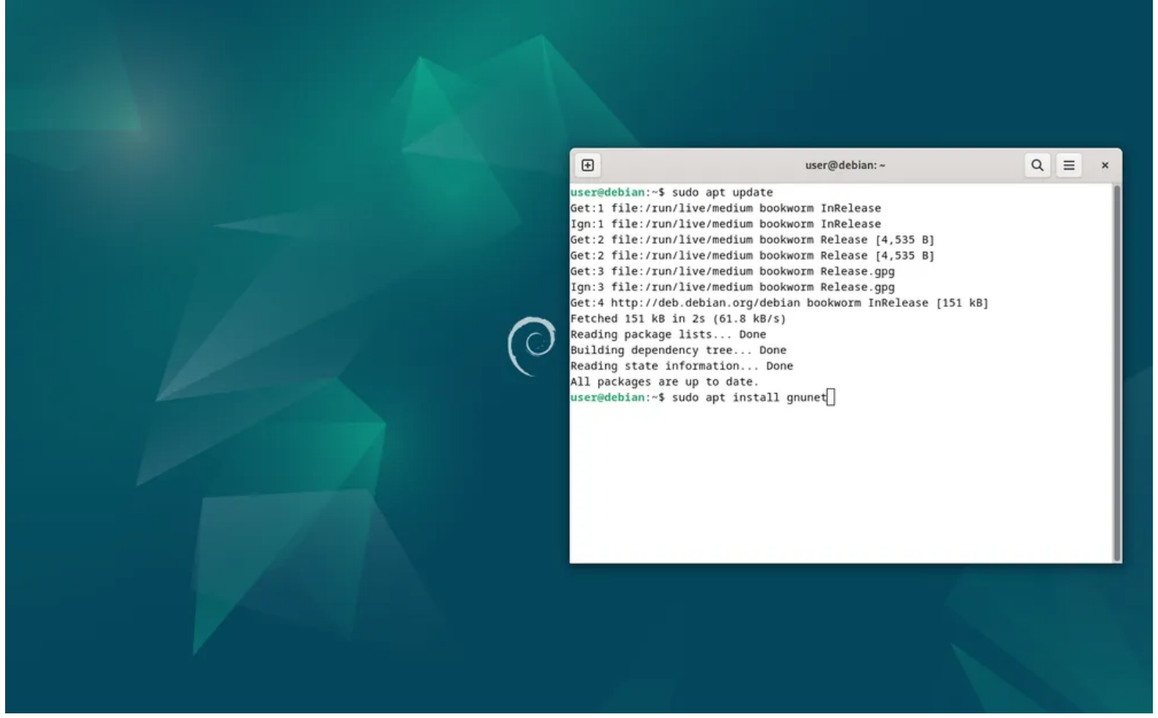


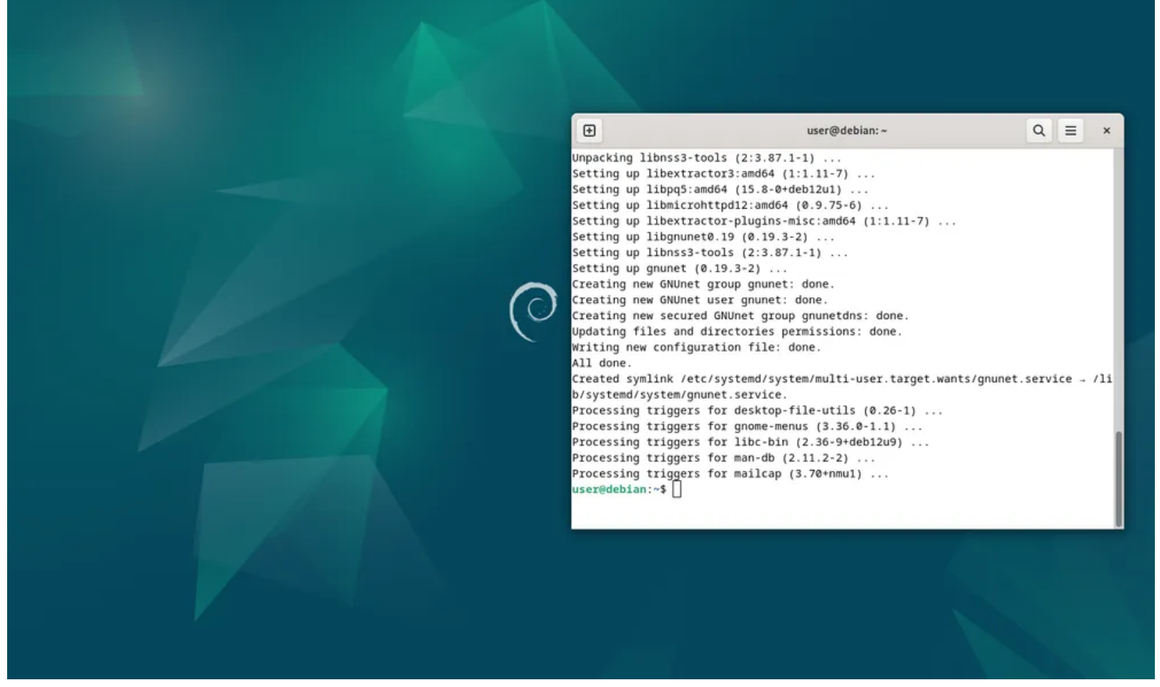
3. sudo apt update 입력하고 엔터.



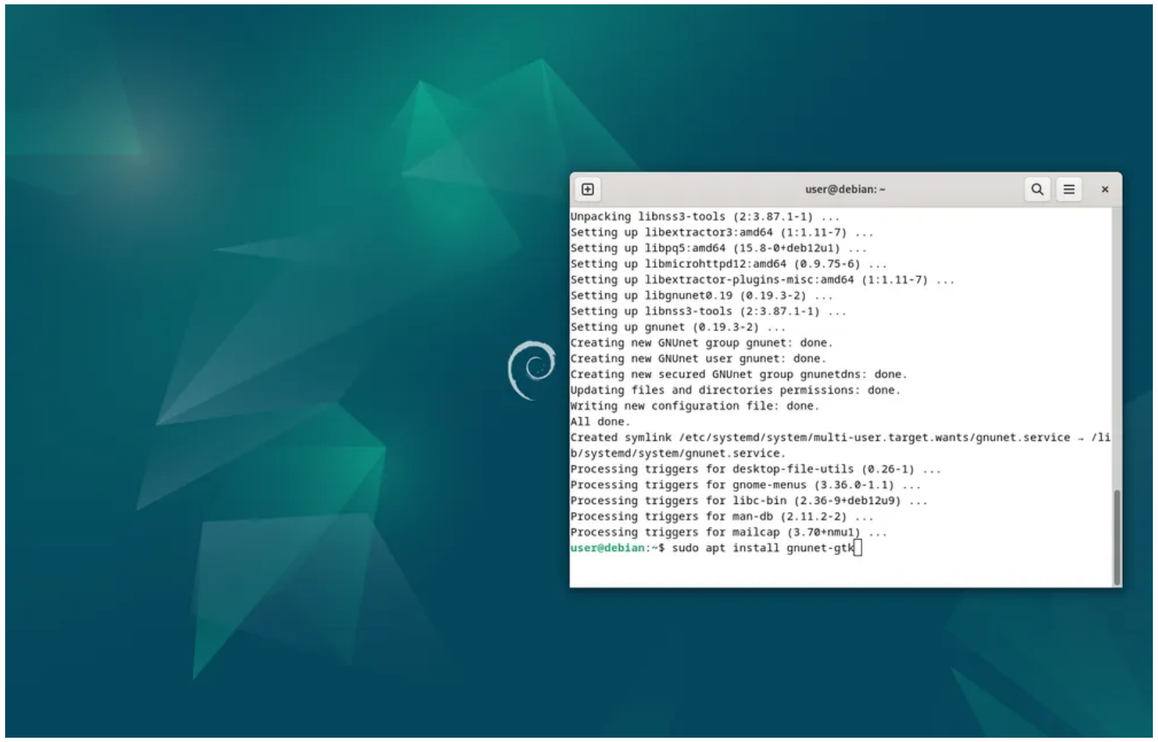

user@debian: ~
Ign:3 file:/run/live/medium bookworm Release.gpg
Get:4 http://deb.debian.org/debian bookworm InRelease [151 kB]
Fetched 151 kB in 2s (61.8 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
user@debian:~$ sudo apt install gnunet
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libextractor-plugins-misc libextractor3 libgnunet0.19 libmicrohttpd12
libnss3-tools libpq5
Suggested packages:
miniupnpc texlive libextractor-java libextractor-plugins-all
python3-extractor
The following NEW packages will be installed:
gnunet libextractor-plugins-misc libextractor3 libgnunet0.19 libmicrohttpd12
libnss3-tools libpq5
0 upgraded, 7 newly installed, 0 to remove and 0 not upgraded.
Need to get 5,633 kB of archives.
After this operation, 23.7 MB of additional disk space will be used.
Do you want to continue? [Y/n] y

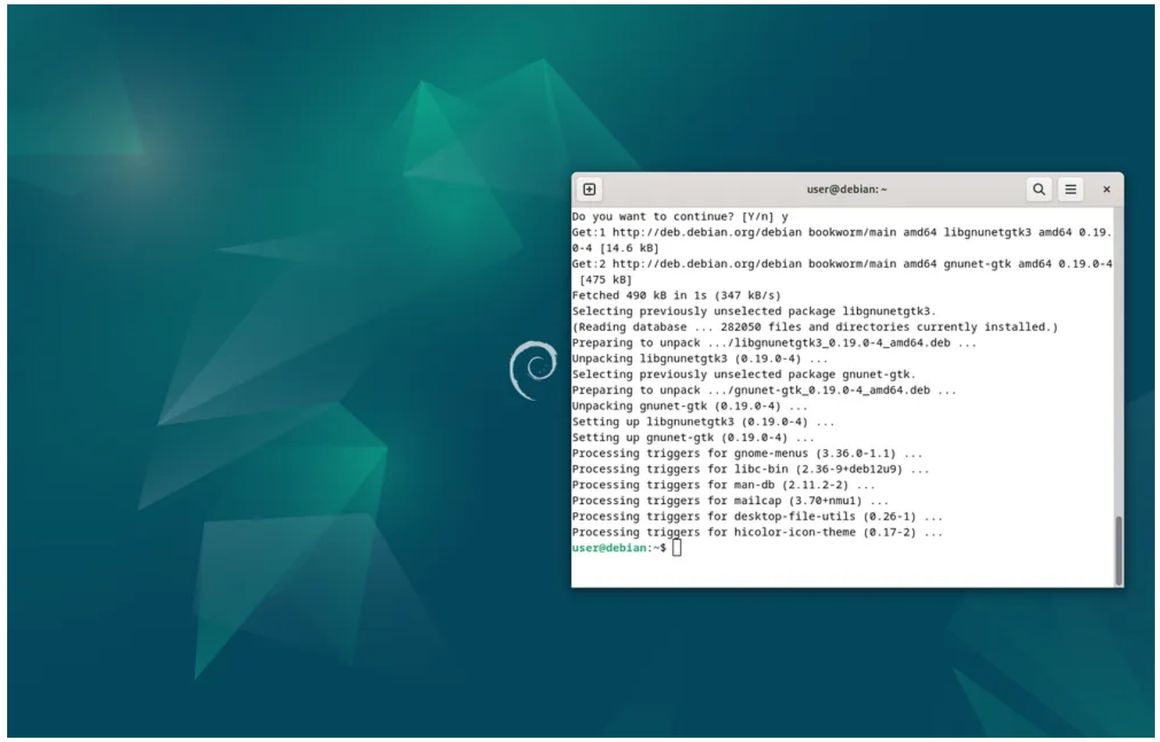
4. sudo apt install gnunet 입력하고 엔터.

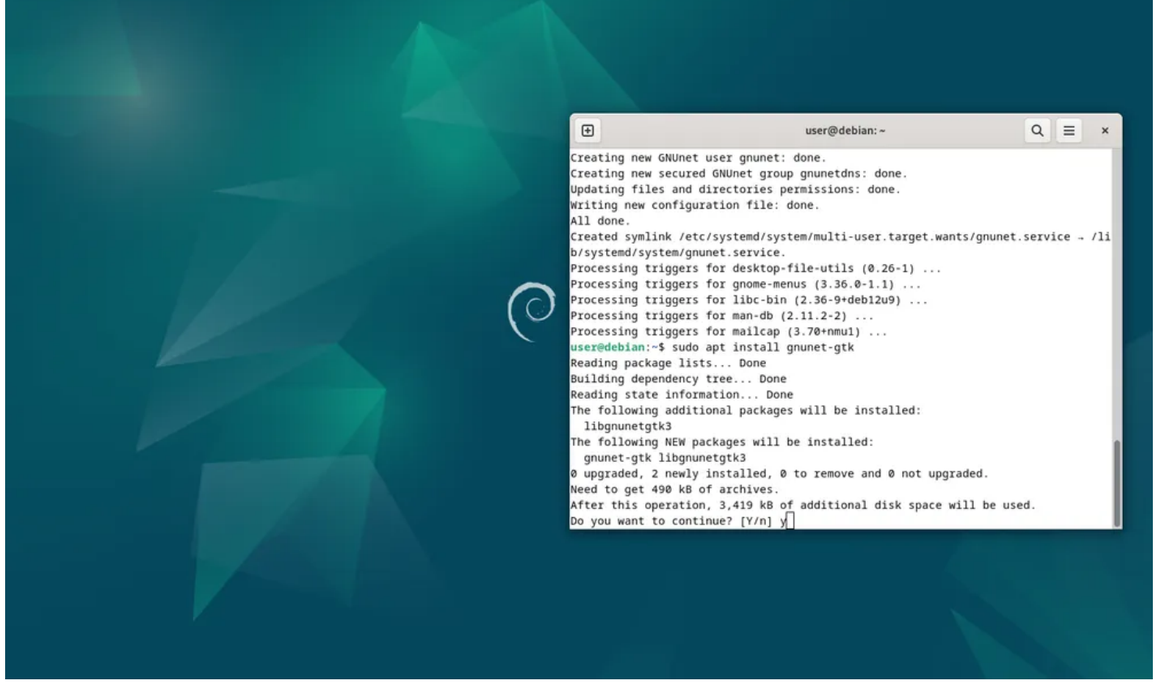

user@debian: ~
user@debian:~$ sudo apt update
Get:1 file:/run/live/medium bookworm InRelease
Ign:1 file:/run/live/medium bookworm InRelease
Get:2 file:/run/live/medium bookworm Release [4,535 B]
Get:2 file:/run/live/medium bookworm Release [4,535 B]
Get:3 file:/run/live/medium bookworm Release.gpg
Ign:3 file:/run/live/medium bookworm Release.gpg
Get:4 http://deb.debian.org/debian bookworm InRelease [151 kB]
Fetched 151 kB in 2s (61.8 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
user@debian:~$ sudo apt install gnunet


user@debian: ~
Unpacking libnss3-tools (2:3.87.1-1) ...
Setting up libextractor3:amd64 (1:1.11-7) ...
Setting up libpq5:amd64 (15.8-0+deb12u1) ...
Setting up libmicrohttpd12:amd64 (0.9.75-6) ...
Setting up libextractor-plugins-misc:amd64 (1:1.11-7) ...
Setting up libgnunet0.19 (0.19.3-2) ...
Setting up libnss3-tools (2:3.87.1-1) ...
Setting up gnunet (0.19.3-2) ...
Creating new GNUnet group gnunet: done.
Creating new GNUnet user gnunet: done.
Creating new secured GNUnet group gnunetdns: done.
Updating files and directories permissions: done.
Writing new configuration file: done.
All done.
Created symlink /etc/systemd/system/multi-user.target.wants/gnunet.service → /lib/systemd/system/gnunet.service.
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for gnome-menus (3.36.0-1.1) ...
Processing triggers for libc-bin (2.36-9+deb12u9) ...
Processing triggers for man-db (2.11.2-2) ...
Processing triggers for mailcap (3.70+nmu1) ...
user@debian:~$

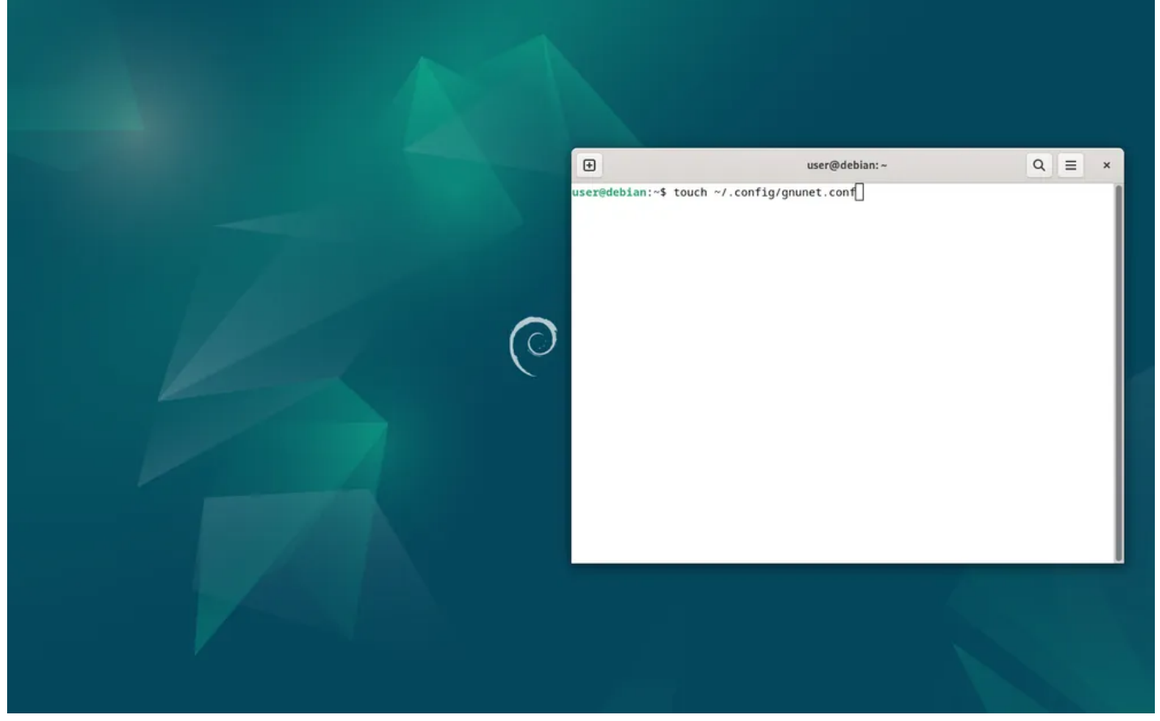
5. sudo apt install gnunet-gtk 입력하고 엔터.

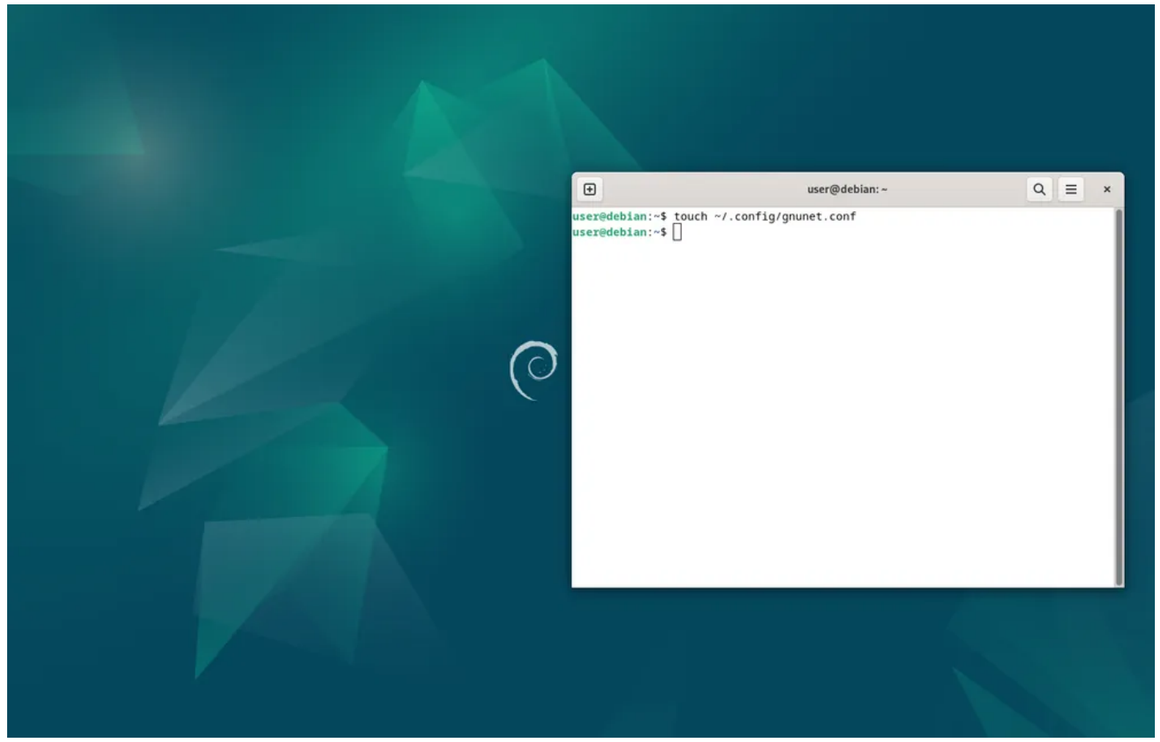

user@debian: ~
Unpacking libnss3-tools (2:3.87.1-1) ...
Setting up libextractor3:amd64 (1:1.11-7) ...
Setting up libpq5:amd64 (15.8-0+deb12u1) ...
Setting up libmicrohttpd12:amd64 (0.9.75-6) ...
Setting up libextractor-plugins-misc:amd64 (1:1.11-7) ...
Setting up libgnunet0.19 (0.19.3-2) ...
Setting up libnss3-tools (2:3.87.1-1) ...
Setting up gnunet (0.19.3-2) ...
Creating new GNUnet group gnunet: done.
Creating new GNUnet user gnunet: done.
Creating new secured GNUnet group gnunetdns: done.
Updating files and directories permissions: done.
Writing new configuration file: done.
All done.
Created symlink /etc/systemd/system/multi-user.target.wants/gnunet.service → /lib/systemd/system/gnunet.service.
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for gnome-menus (3.36.0-1.1) ...
Processing triggers for libc-bin (2.36-9+deb12u9) ...
Processing triggers for man-db (2.11.2-2) ...
Processing triggers for mailcap (3.70+nmu1) ...
user@debian:~$ sudo apt install gnunet-gtk


user@debian: ~
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian bookworm/main amd64 libgnunetgtk3 amd64 0.19.0-4 [14.6 kB]
Get:2 http://deb.debian.org/debian bookworm/main amd64 gnunet-gtk amd64 0.19.0-4 [475 kB]
Fetched 490 kB in 1s (347 kB/s)
Selecting previously unselected package libgnunetgtk3.
(Reading database ... 282050 files and directories currently installed.)
Preparing to unpack .../libgnunetgtk3_0.19.0-4_amd64.deb ...
Unpacking libgnunetgtk3 (0.19.0-4) ...
Selecting previously unselected package gnunet-gtk.
Preparing to unpack .../gnunet-gtk_0.19.0-4_amd64.deb ...
Unpacking gnunet-gtk (0.19.0-4) ...
Setting up libgnunetgtk3 (0.19.0-4) ...
Setting up gnunet-gtk (0.19.0-4) ...
Processing triggers for gnome-menus (3.36.0-1.1) ...
Processing triggers for libc-bin (2.36-9+deb12u9) ...
Processing triggers for man-db (2.11.2-2) ...
Processing triggers for mailcap (3.70+nmu1) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
user@debian:~$

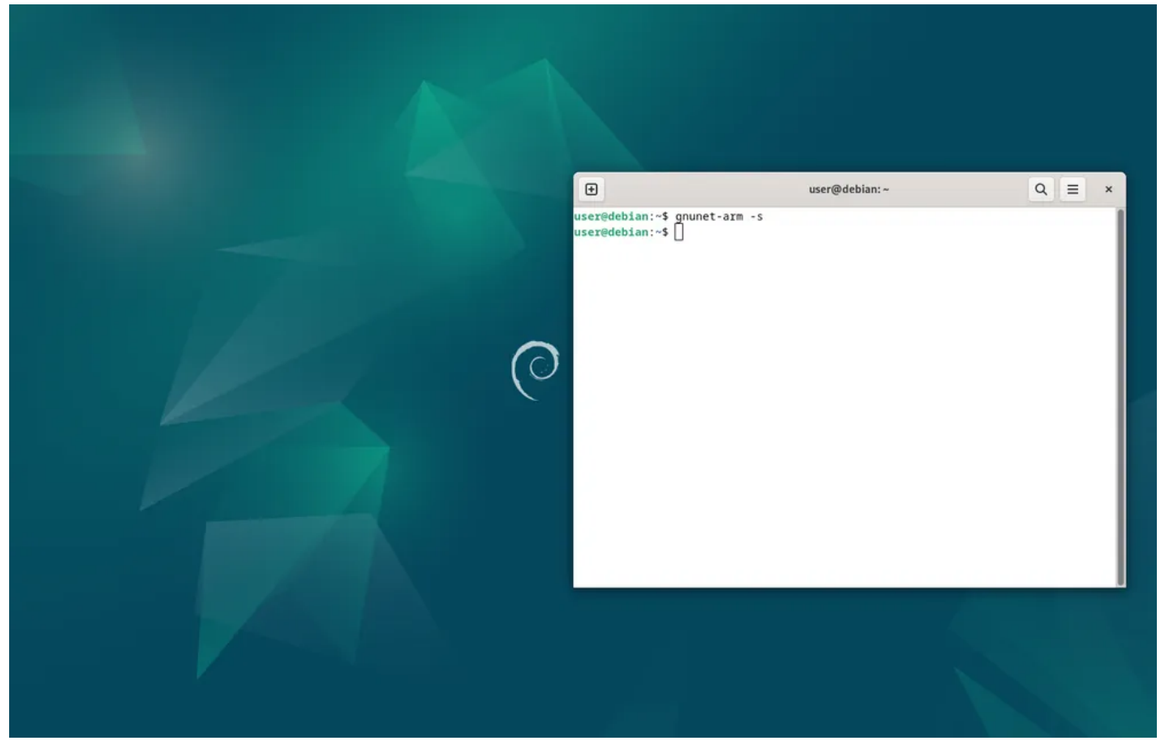

user@debian: ~
Creating new GNUnet user gnunet: done.
Creating new secured GNUnet group gnunetdns: done.
Updating files and directories permissions: done.
Writing new configuration file: done.
All done.
Created symlink /etc/systemd/system/multi-user.target.wants/gnunet.service → /lib/systemd/system/gnunet.service.
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for gnome-menus (3.36.0-1.1) ...
Processing triggers for libc-bin (2.36-9+deb12u9) ...
Processing triggers for man-db (2.11.2-2) ...
Processing triggers for mailcap (3.70+nmu1) ...
user@debian:~$ sudo apt install gnunet-gtk
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libgnunetgtk3
The following NEW packages will be installed:
  gnunet-gtk libgnunetgtk3
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 490 kB of archives.
After this operation, 3,419 kB of additional disk space will be used.
Do you want to continue? [Y/n] y

6. touch ~/.config/gnunet.conf 입력하고 엔터.

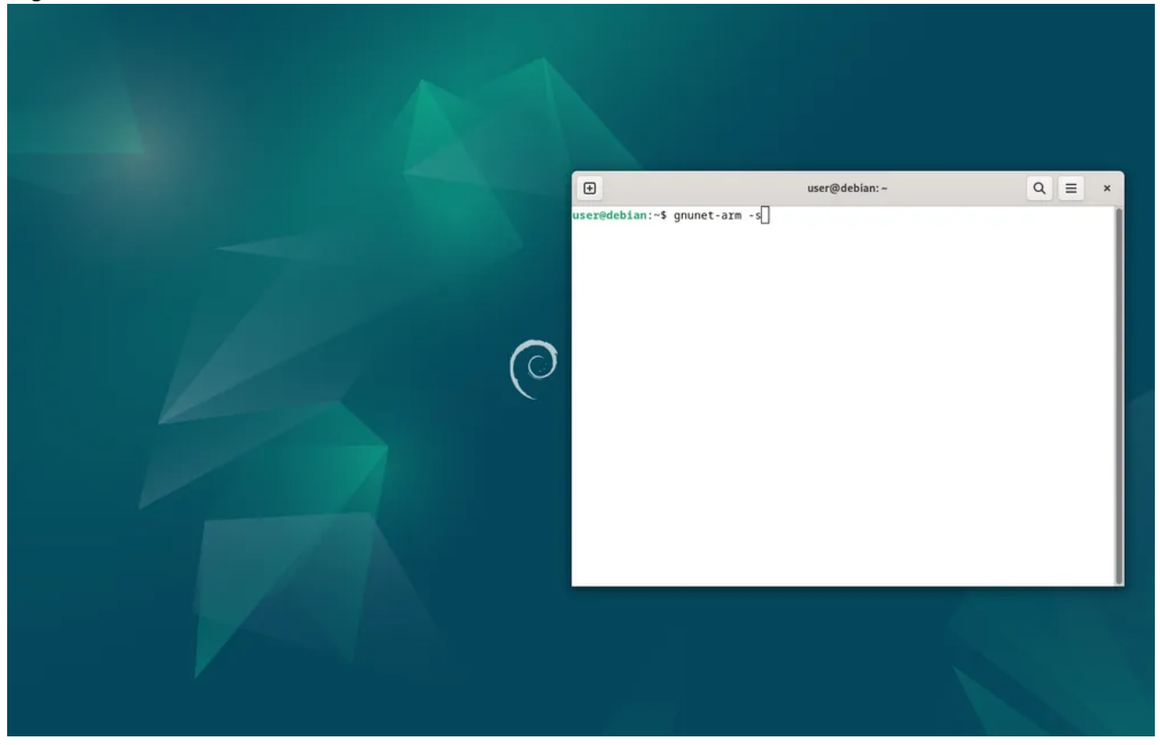


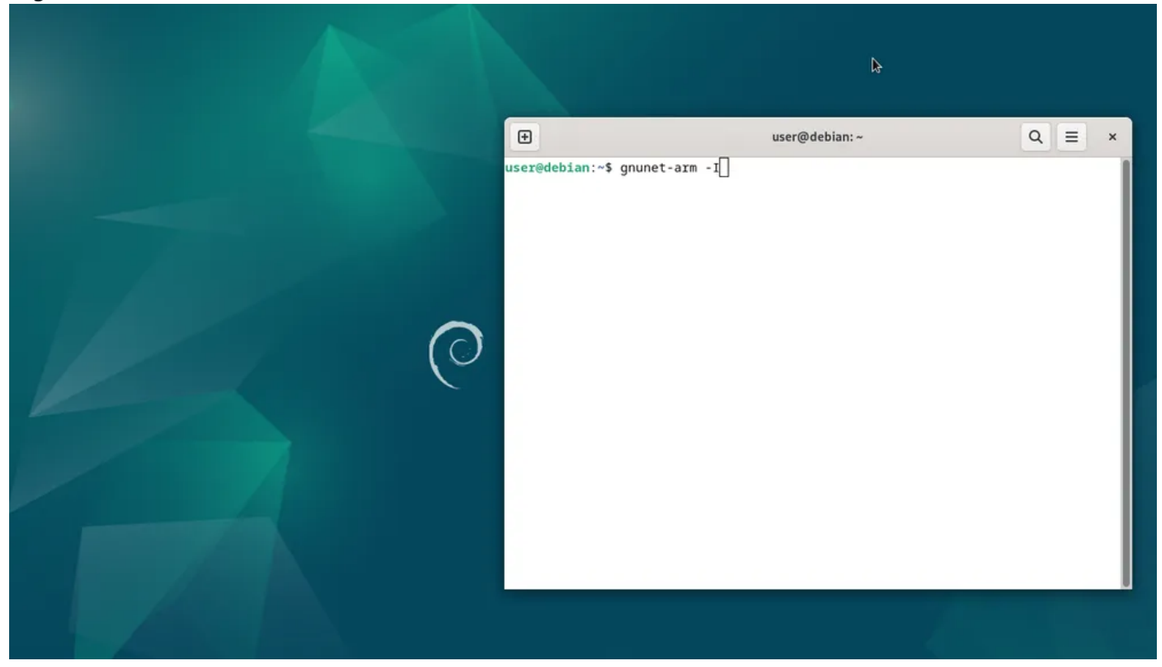


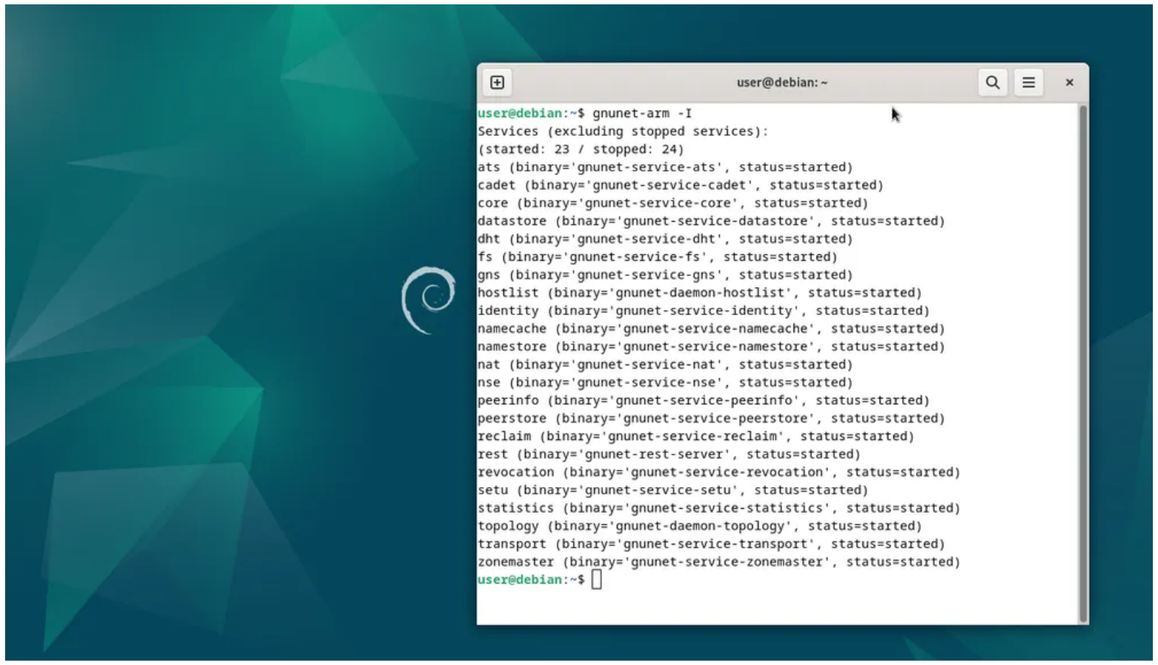
7. gnunet-arm -s 입력하고 엔터. GNUnet을 켠다.



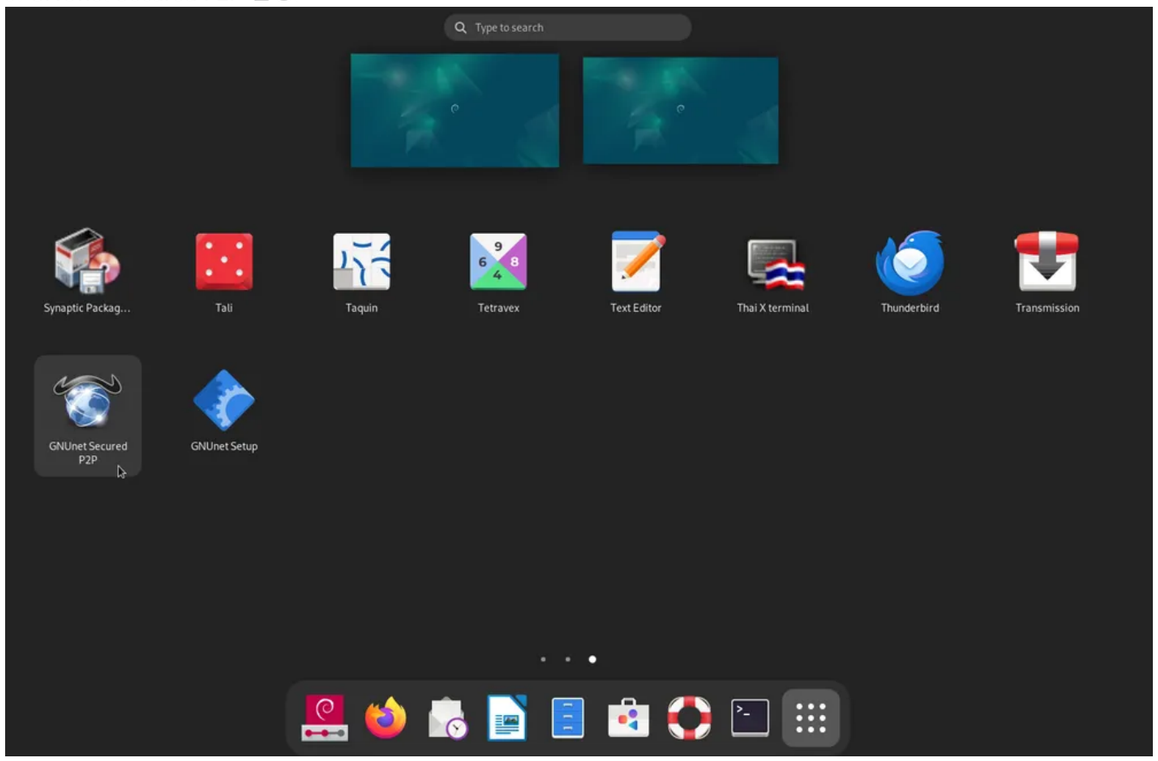
8. gnunet-arm -I 입력하고 엔터. 실행 중인 GNUnet 서비스를 확인한다.



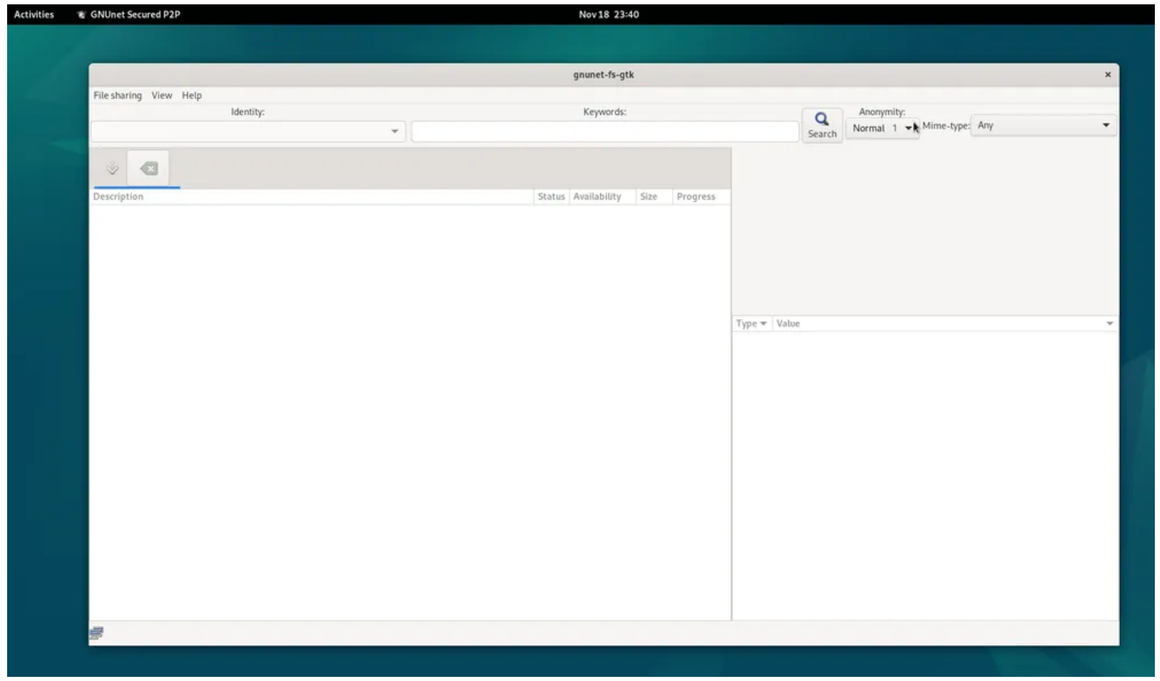




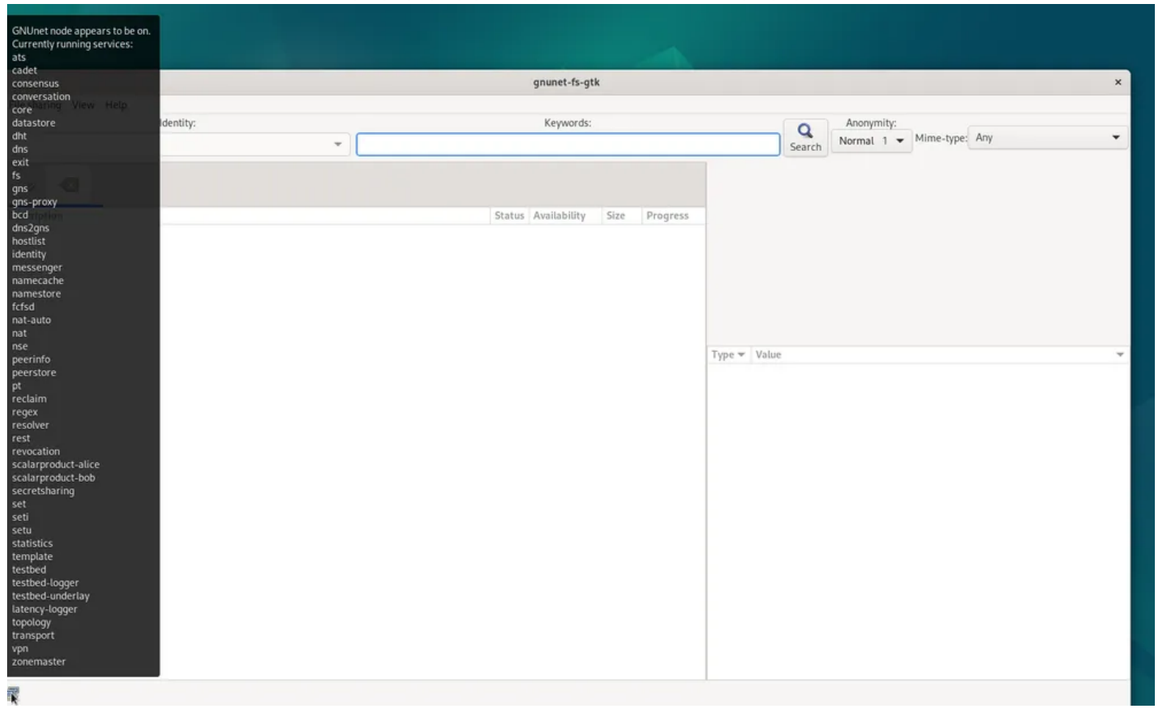
9. GNUnet Secured P2P 실행.



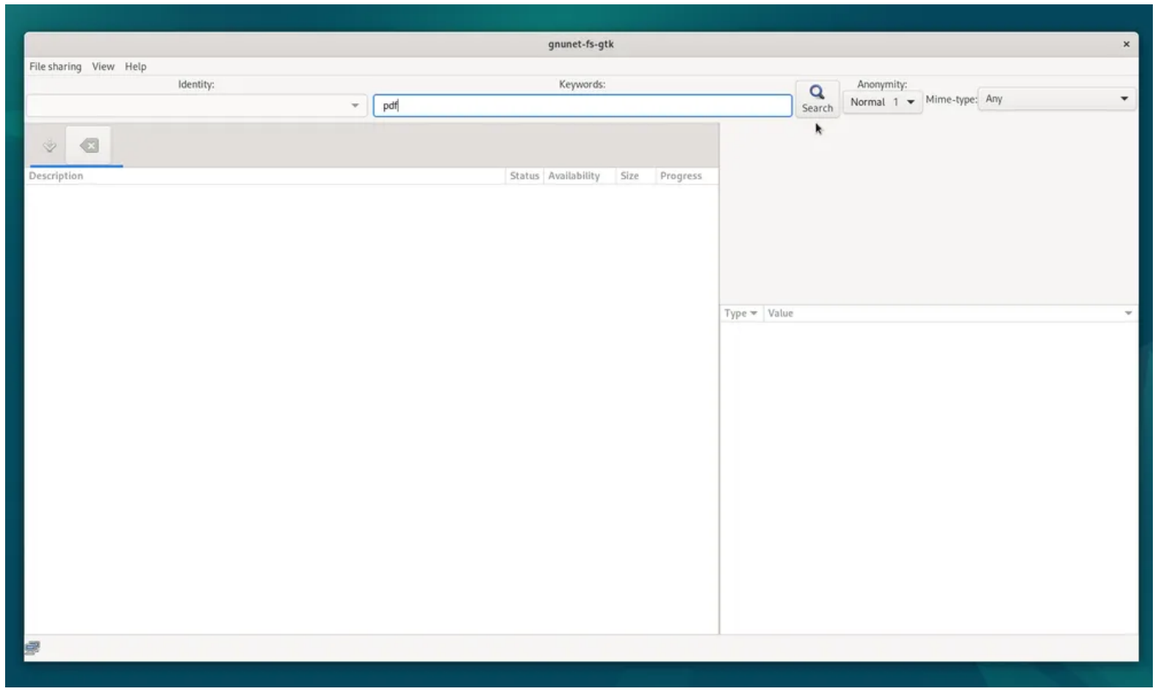
10. GNUnet Secured P2P의 전체 모습이다.



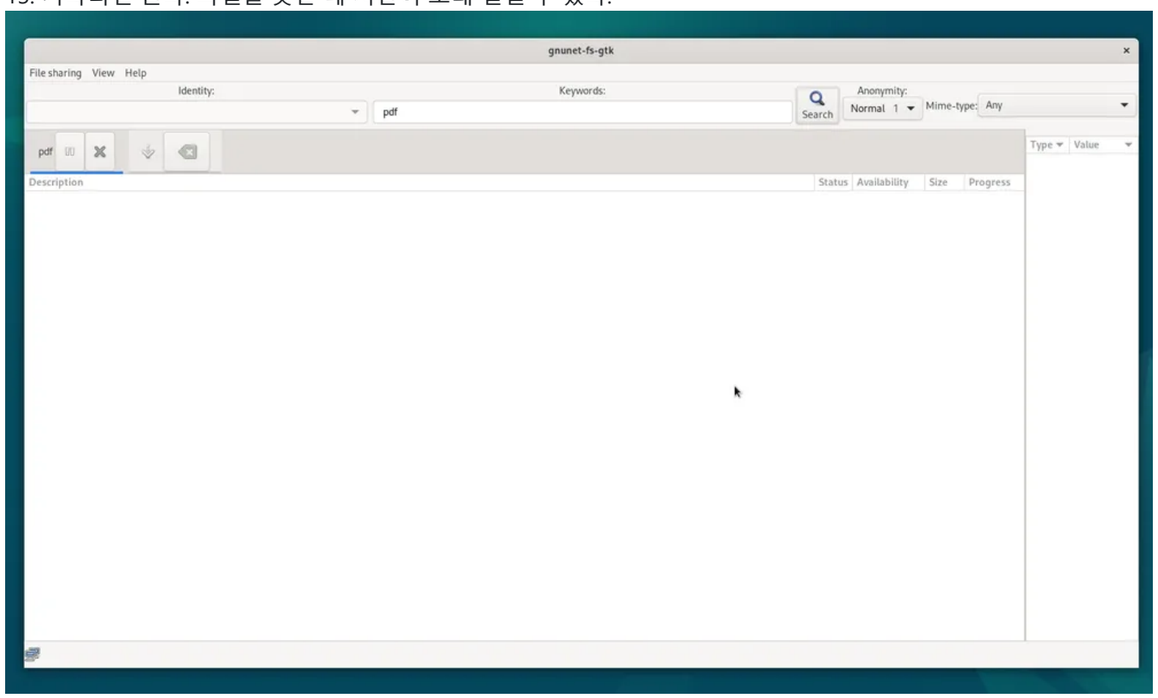
11. GNUnet Secured P2P의 창 왼쪽 아래에 마우스 커서를 대면 GNUnet이 켜져 있는지 확인할 수 있다.



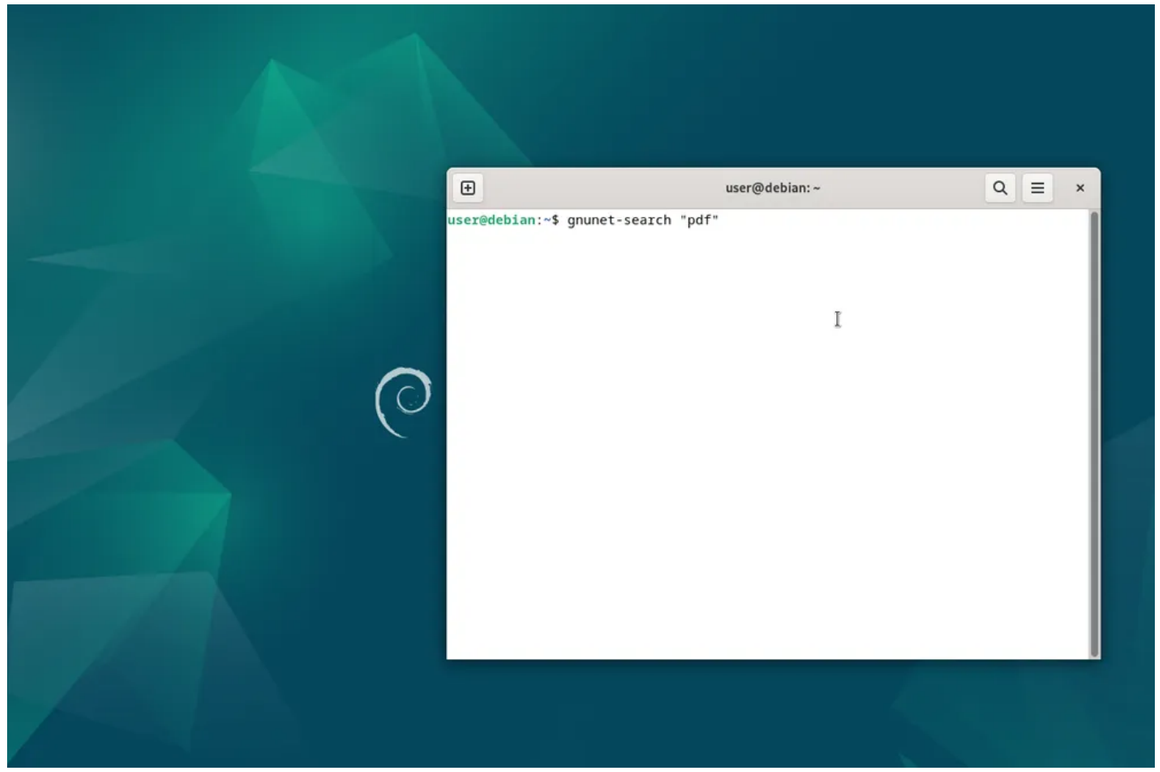
12. 원하는 파일을 검색할 수 있다.

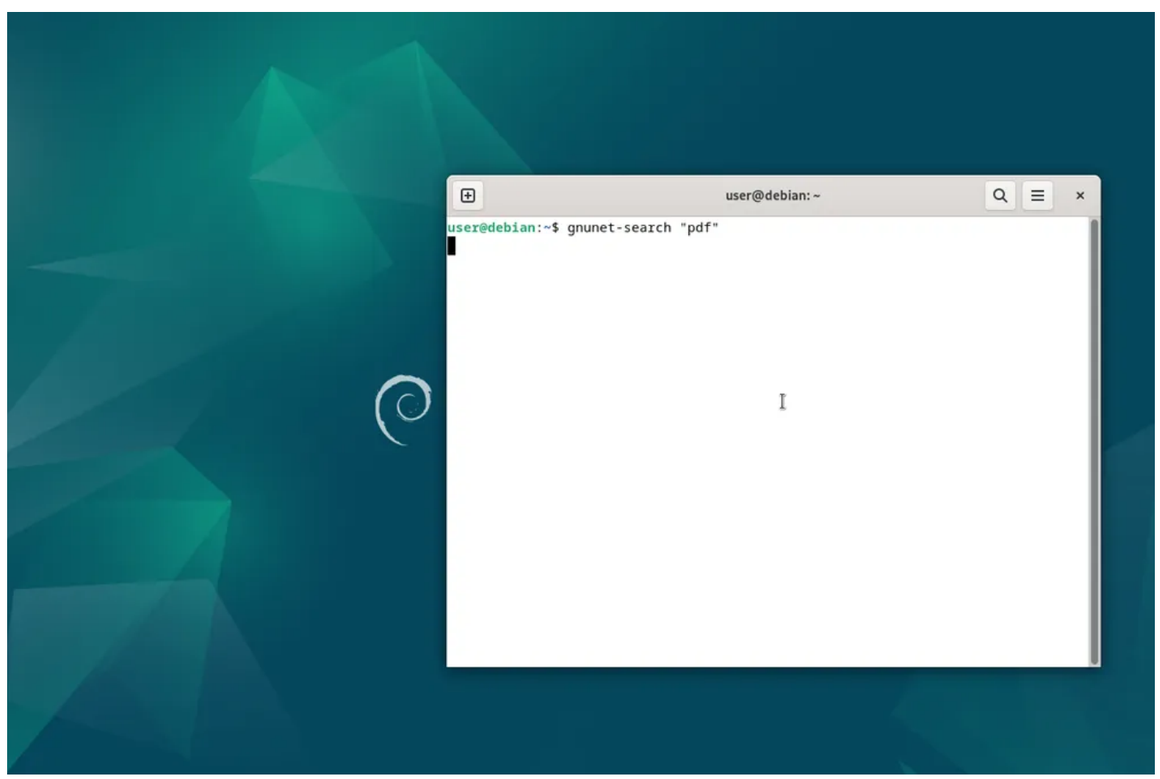


13. 기다리면 된다. 파일을 찾는 데 시간이 오래 걸릴 수 있다.

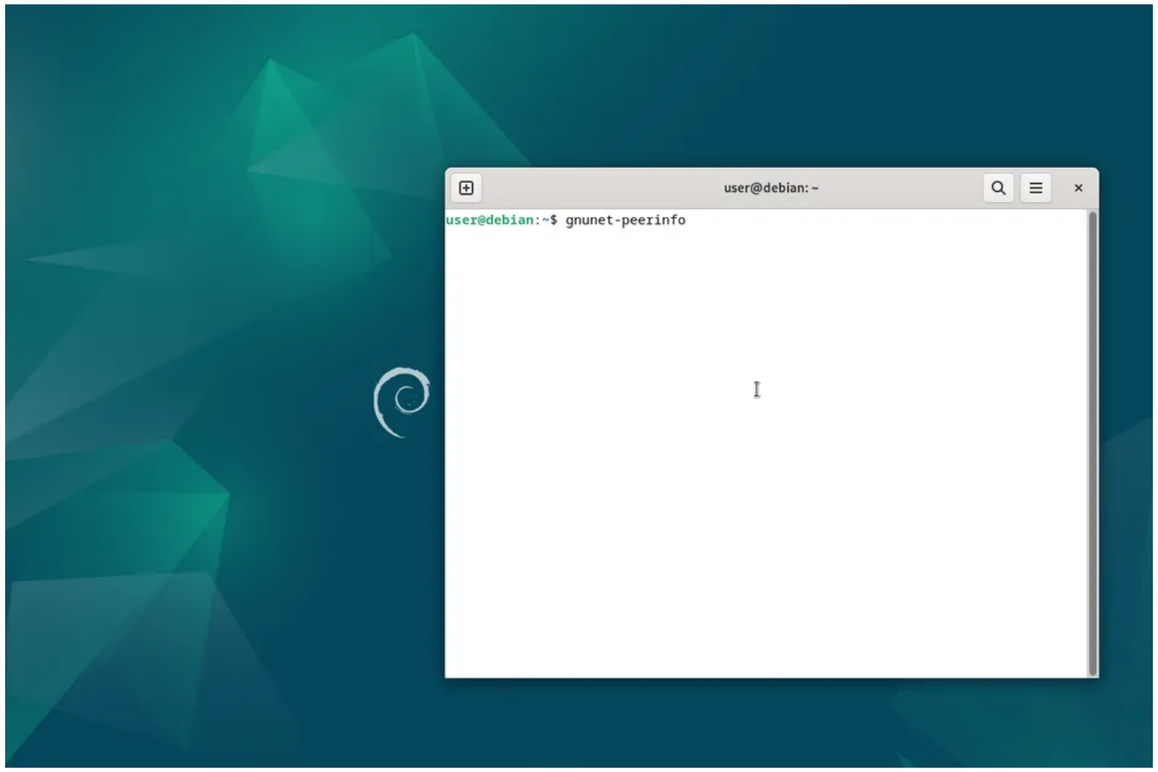


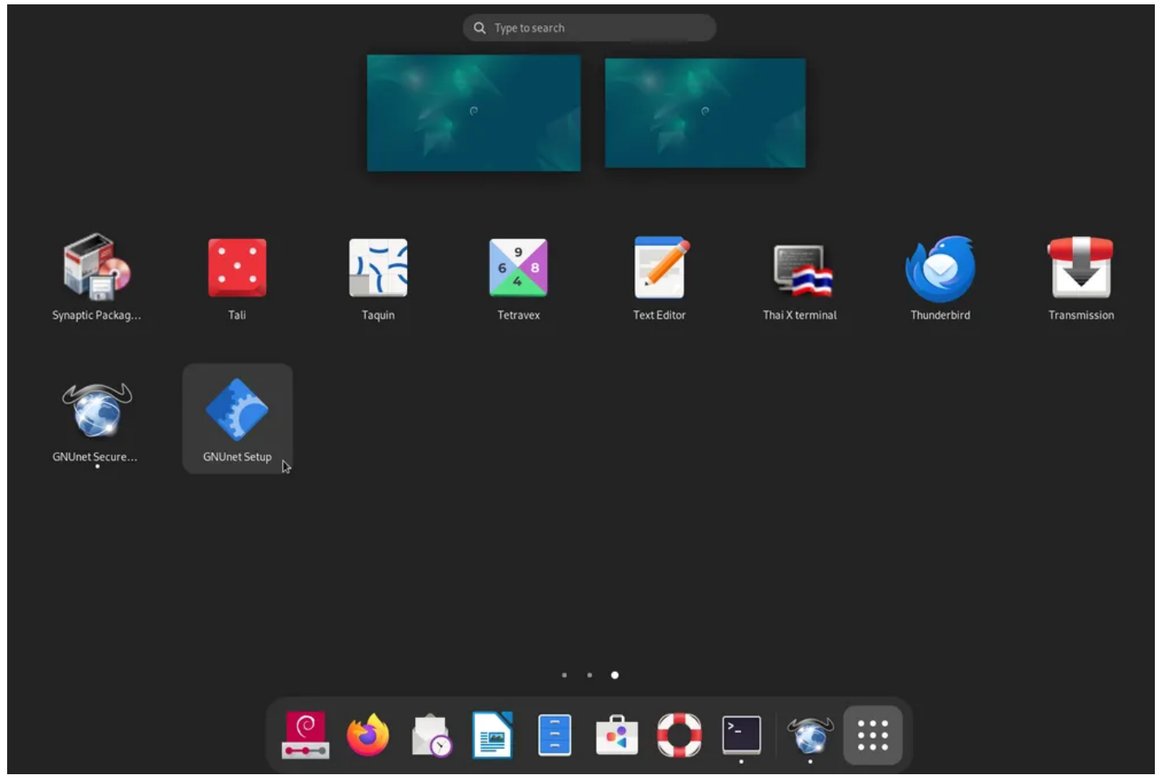
14. 터미널에서 gnunet-search "keyword"를 입력하여 파일을 검색할 수도 있다.

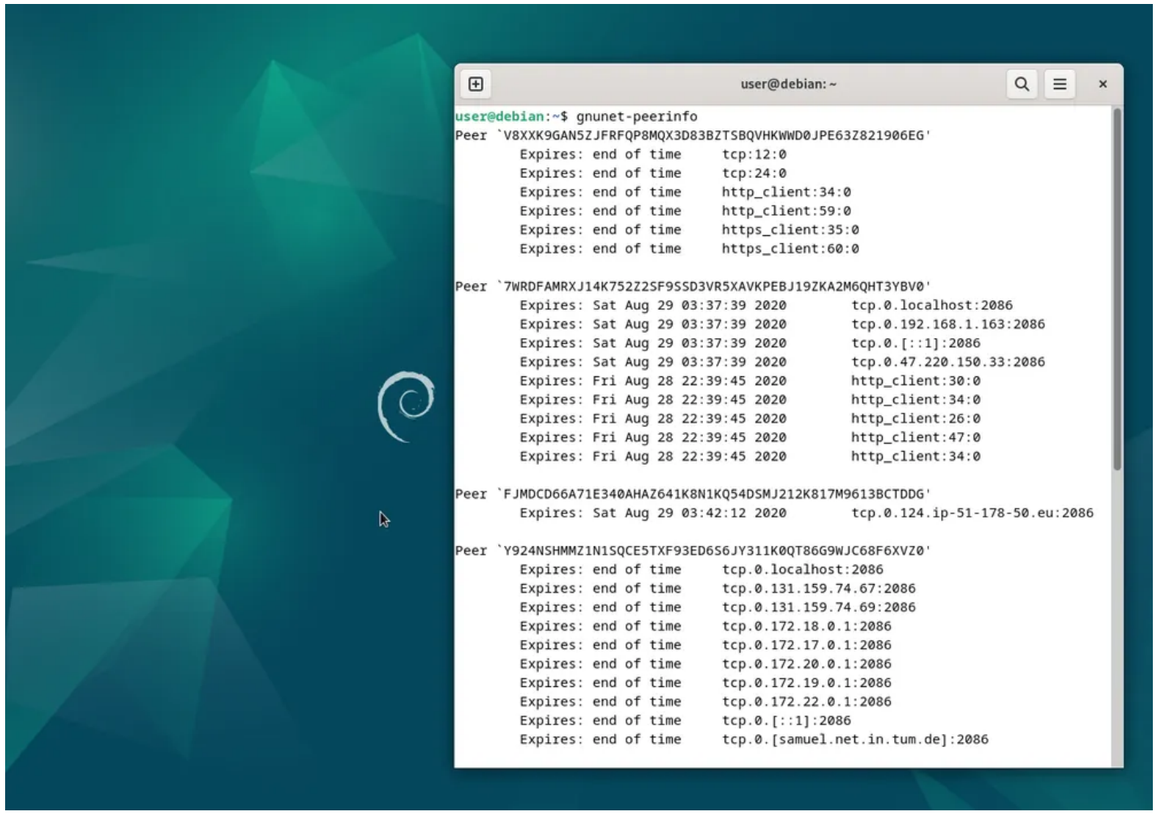




15. gnunet-peerinfo 입력하고 엔터. 나와 연결되어 있는 GNUnet 노드를 확인할 수 있다.

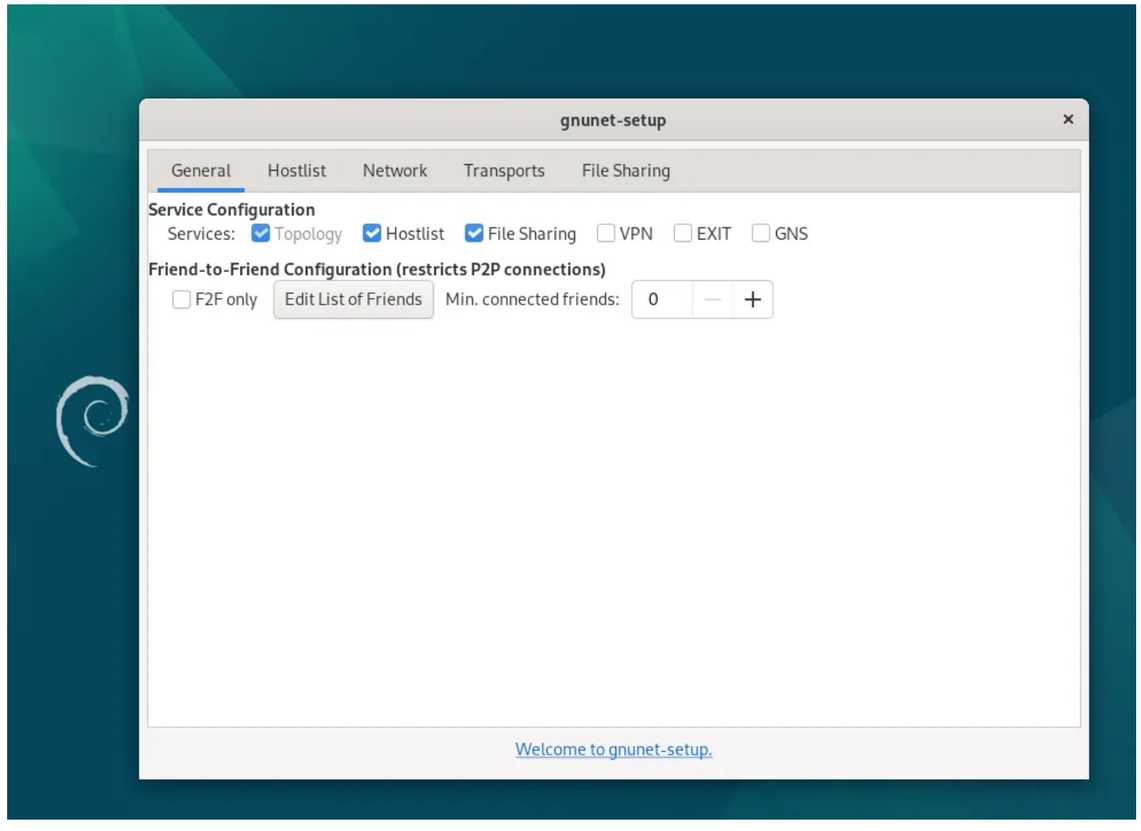





user@debian: ~
user@debian:~$ gnunet-peerinfo
Peer `V8XXK9GAN5ZJFRFQP8MQX3D83BZTSBQVHKWWD0JPE63Z821906EG'
Expires: end of time tcp:12:0
Expires: end of time tcp:24:0
Expires: end of time http_client:34:0
Expires: end of time http_client:59:0
Expires: end of time https_client:35:0
Expires: end of time https_client:60:0
Peer `7WRDFAMRXJ14K752Z2SF9SSD3VR5XAVKPEBJ19ZKA2M6QHT3YBV0'
Expires: Sat Aug 29 03:37:39 2020 tcp.0.localhost:2086
Expires: Sat Aug 29 03:37:39 2020 tcp.0.192.168.1.163:2086
Expires: Sat Aug 29 03:37:39 2020 tcp.0.[::1]:2086
Expires: Sat Aug 29 03:37:39 2020 tcp.0.47.220.150.33:2086
Expires: Fri Aug 28 22:39:45 2020 http_client:30:0
Expires: Fri Aug 28 22:39:45 2020 http_client:34:0
Expires: Fri Aug 28 22:39:45 2020 http_client:26:0
Expires: Fri Aug 28 22:39:45 2020 http_client:47:0
Expires: Fri Aug 28 22:39:45 2020 http_client:34:0
Peer `FJMDCD66A71E340AHAZ641K8N1KQ54DSMJ212K817M9613BCTDDG'
Expires: Sat Aug 29 03:42:12 2020 tcp.0.124.ip-51-178-50.eu:2086
Peer `Y924NSHMMZ1N1SQCE5TXF93ED6S6JY311K0QT86G9WJC68F6XVZ0'
Expires: end of time tcp.0.localhost:2086
Expires: end of time tcp.0.131.159.74.67:2086
Expires: end of time tcp.0.131.159.74.69:2086
Expires: end of time tcp.0.172.18.0.1:2086
Expires: end of time tcp.0.172.17.0.1:2086
Expires: end of time tcp.0.172.20.0.1:2086
Expires: end of time tcp.0.172.19.0.1:2086
Expires: end of time tcp.0.172.22.0.1:2086
Expires: end of time tcp.0.[::1]:2086
Expires: end of time tcp.0.[samuel.net.in.tum.de]:2086

16. GNUnet Setup 실행.

17. 여러 설정이 있다.



gnunet-setup

General | Hostlist | Network | Transports | File Sharing

Hostlist Configuration (for bootstrapping the network)

☑ Use Hostlists to bootstrap ☐ Learn Servers from P2P Network

☐ Run Hostlist Server

Known Hostlist Servers:

URL
http://v15.gnunet.org/hostlist
https://gnunet.io/hostlist

Proxy configuration

- (•) no proxy
- ( ) HTTP proxy
- ( ) HTTP 1.0 proxy

Proxy type:

- ( ) SOCKS v4 proxy
- ( ) SOCKS v4a proxy
- ( ) SOCKS v5 proxy
- ( ) SOCKS v5 proxy with hostname

Proxy hostname:

Proxy username:

Proxy password:

Welcome to gnunet-setup.

gnunet-setup

General | Hostlist | Network | Transports | File Sharing

Transport Configuration

Plugins to use: ☑ TCP ☐ UDP ☐ HTTP Client ☐ HTTP Server ☐ HTTPS Client ☐ HTTPS Server ☐ WLAN

TCP

Bind to port: 2086 − + Use Port "0" to only allow outgoing TCP connections

Advertised port: 2086 − + External port visible on our public IP address after mappings by NAT/firewalls

Test configuration

Welcome to gnunet-setup.

gnunet-setup

General | Hostlist | Network | Transports | File Sharing

Bandwidth Configuration

Max. download bandwidth (B/s): 5000 − +

Max. upload bandwidth (B/s): 1024 − +

Welcome to gnunet-setup.

gnunet-setup

General | Hostlist | Network | Transports | File Sharing

File Sharing Options

☑ Enable unsolicited content transmission from this peer ☑ Enable caching content at this peer

Configure Datastore (persistent storage)

Database Backend to use: (•) sqLite ( ) MySQL ( ) Postgres Quota (bytes): 1000000 − +

sqLite

No setup required.

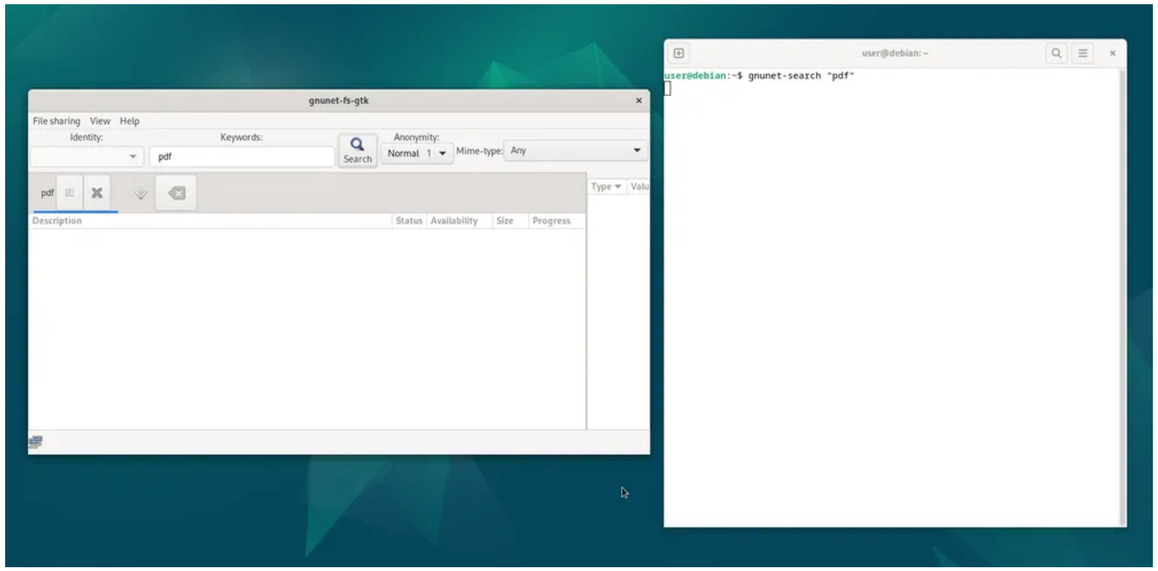
Configure Datacache (temporary storage)

Datacache: ( ) sqLite (•) Memory ( ) Postgres Quota (bytes): 65536 − +

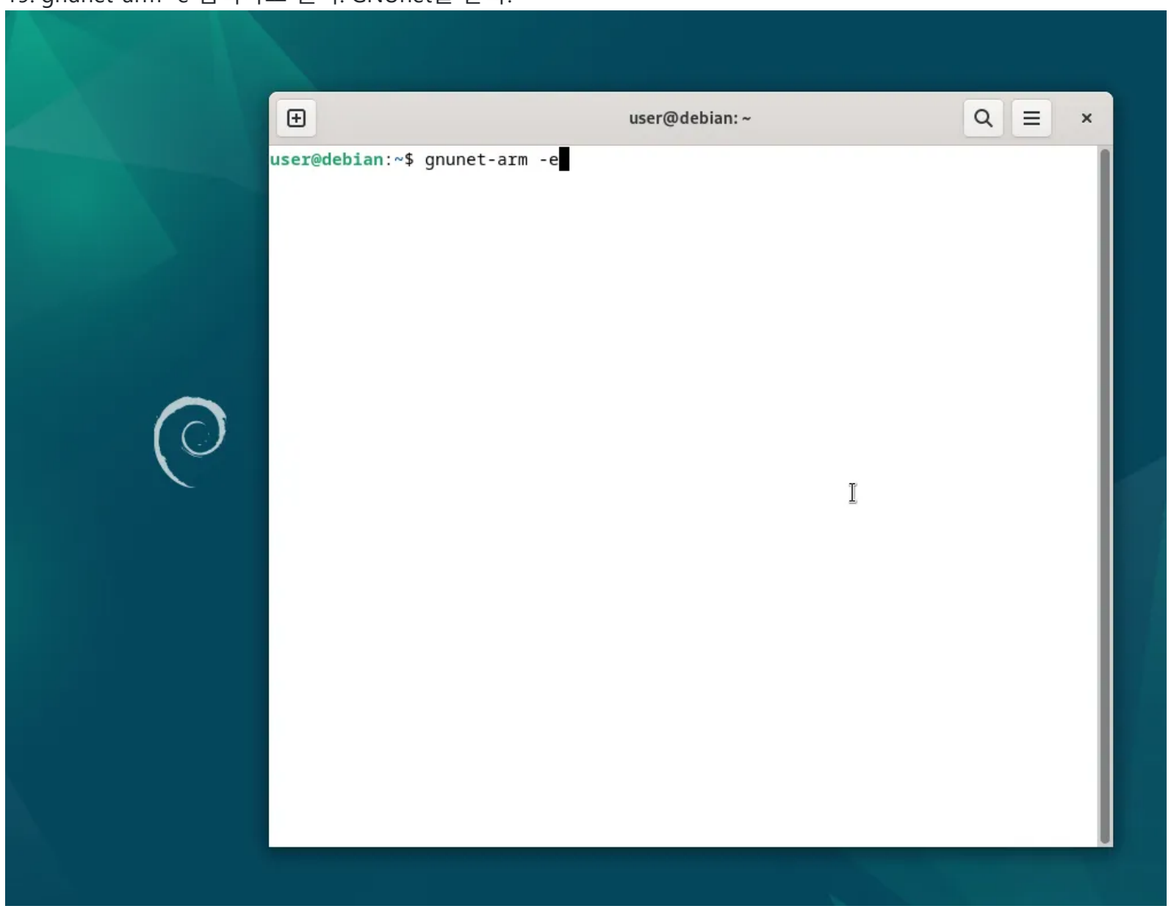
sqLite

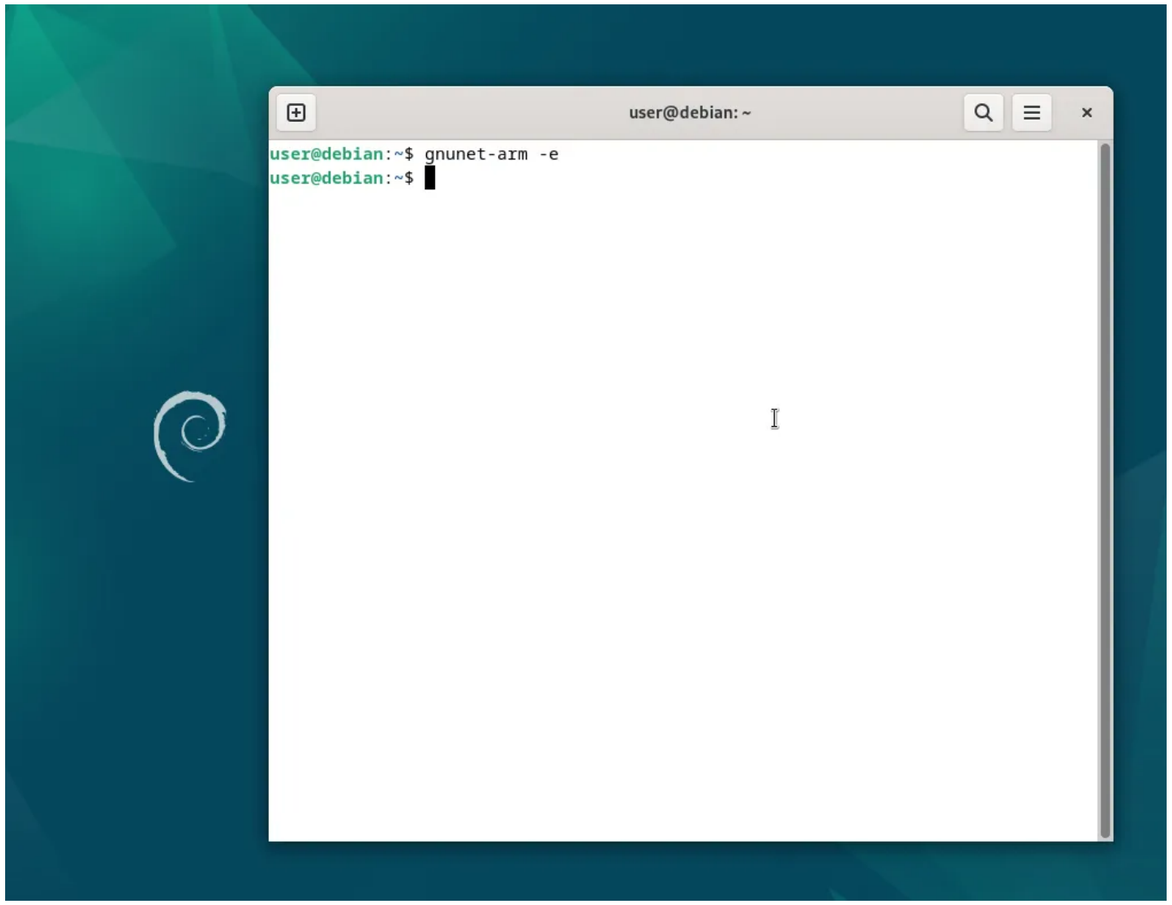
Welcome to gnunet-setup.

18. 파일을 찾는 데 오랜 시간이 걸릴 수 있다.

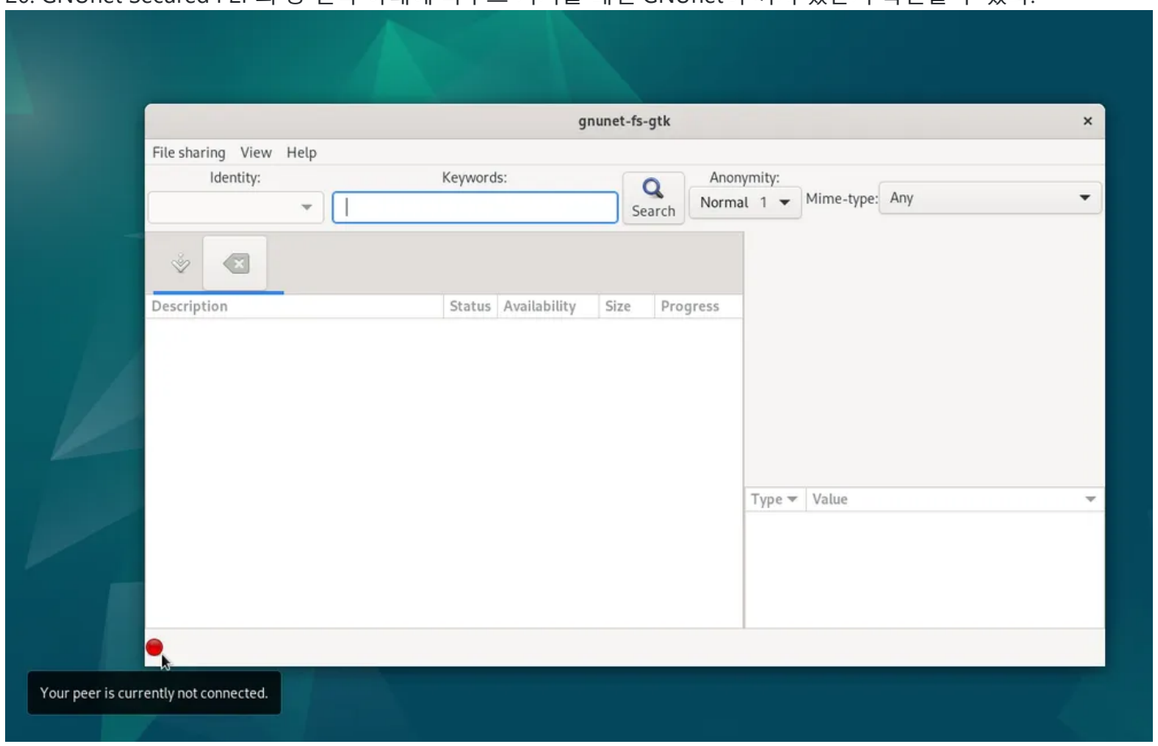


19. gnunet-arm -e 입력하고 엔터. GNUnet을 끈다.





20. GNUnet Secured P2P의 창 왼쪽 아래에 마우스 커서를 대면 GNUnet이 꺼져 있는지 확인할 수 있다.



지금까지 데비안에서 GNUnet을 설치하고 이용하는 방법을 알아보았다.

3. 한계

> 너무 복잡하고 설명서도 끔찍합니다. 복잡하기 때문에 보안이 어렵습니다. 보안이 어렵기 때문에 보안을 제공하지 못합니다. RetroShare나 I2P와 비교하면 구식 스타일입니다. 둘 다 관리하기 쉬운 그래픽 인터페이스를 가지고 있고 보안을 부여하려면 "관리하기 쉬움"이 필요합니다.
> 복잡성과 잘못된 설명서는 보안의 최악의 적이며, gnunet은 바로 이러한 실수의 예입니다. 관리하기 쉽지 않기 때문에 안전할 수 없습니다. 누군가가 안전하게 실행할 수 있다 하더라도 우연히 시작할 수 있었던 누군가의 네트워크에서 끝날 것입니다.
> 저는 그것을 살펴보았고, 시행착오로 주말을 보냈습니다(로깅이 전혀 유용하지 않기 때문에). 그리고 나서 요점을 깨달았습니다. 너무 복잡하고 로깅은 아무 말도 하지 않으며 항상 우연히 설치한 사람들과 함께 어떤 네트워크에 빠지기 때문에 안전할 수 없습니다. 저는 전적으로 찬성입니다. 이것에 시간을 낭비하지 마십시오.
> 저는 gnunet이 다크넷을 설계하는 데 사용되어서는 안 될 나쁜 관행의 절대적인 모음이라고 말하고 싶습니다: 문서 부족, 난독화되거나 존재하지 않는 로그, 과도한 복잡성, 관리 도구 없음. 다크넷을 하지 않는 방법을 배우기 위해서입니다.
>
> It is too complex, and the documentation is horrible. Being complex, it is hard to secure. Being hard to secure , it is not giving you any security. It is old styled, if compared with RetroShare or I2P, both of which have a graphical interface easy to manage, and "easy to manage" is needed to grant security.
> Complexity and bad documentation are the worst enemies of security, and gnunet is exactly an example of this mistake. It cannot be secure because it cannot be easy to manage. Even if someones were able to make it run safely, then they will end for sure in the same network of somebody which was able to start it just by accident.
> I had a look to it, it costed me a weekend of trials and errors (since logging is not useful at all) and then I got the point: it cannot be safe, because it is too complex, logging says nothing , and you will always fall in some network, together with people which installed it just by accident. Totally down for me. Don't waste your time with this.
> I would say gnunet is the absolute collection of any bad practice should NOT be used to design a darknet: lack of documentation, obfuscated or non-existing logs, overcomplexity, no administration tools. Just to learn how to DON'T do a darknet.
>
> https://www.reddit.com/r/i2p/comments/2iadki/anyone_tried_gnunet_is_it_worth_itno_gnunet_sub/ @

GNUnet은 접근성이 나쁘고 실용성이 부족하여 이용자가 거의 없다.

대신 파일 공유용으로 I2P의 토렌트 기능을 이용하는 것을 권장한다.

4. 억압적인 국가에서의 검열 우회

© 이 문단의 내용 중 전체 또는 일부는 I2P 문서의 r158 판, 10번 문단에서 가져왔습니다. 이전 역사 보러 가기

> If I take your question as "What to do if I'm worried about getting caught running an I2P router in an oppressive regime," and you are worried about the authorities associating your computers with I2P traffic in the long term, and you still want to run an I2P router, then there are generally two solutions:
>
> - Run I2P off-site somewhere it is legal, and access it via an innocuous-seeming form of encrypted connection, such as an SSH connection or an HTTPS connection.
> - Encapsulate your I2P traffic in something legal. If a VPN is legal, then that I guess. If SSH is legal, an SSH tunnel.
>
> But, suppose your adversary is waiting for you to download a particular file that they know you are going to try and download anonymously. If they observe you downloading something that looks like a file of a similar size on your HTTPS tunnel or SSH tunnel or VPN, they're just going to assume that file is what they wanted to catch you with and come after you anyway.
> In fact, at the point where your adversary is willing to go after all I2P users, or all Tor users, or all bittorrent users or TLS users or bitcoin users or whatever, it's impossible to just give people "Settings" that can guarantee they will never be under suspicion. I mean, presumably you got an executable installer from https://i2p.net/, right? So you made DNS requests that say "I'm interested in I2P" you connected to the I2P web site and you downloaded a file about ~18.5 Mb in size. In such a draconian regime, you either get I2P from an unofficial channel, likely a sneakernet channel, or you are already under suspicion. Then you have to re-seed from a channel that can't be monitored easily as well, hopefully your sneakernet guy brought you a fresh reseed file to start with. You get the internet you use it on with a cantenna. You get the idea. In these kinds of very oppressive regimes, technology must be combined with planning, including possibly escape plans.
> Fortunately, only a few countries have this kind of law so far.
> 만약 당신의 질문을 "억압적인 정권 아래에서 I2P 라우터를 운영하다가 적발될까 봐 걱정된다면 어떻게 해야 할까요?"로 이해한다면, 그리고 당국이 당신의 컴퓨터를 I2P 트래픽과 장기적으로 연관시킬까 봐 걱정되지만, 그럼에도 불구하고 I2P 라우터를 운영하고 싶다면 일반적으로 두 가지 해결책이 있습니다.
>
> - I2P를 합법적인 외부 장소에서 운영하고, SSH 연결이나 HTTPS 연결처럼 무해해 보이는 암호화된 연결을 통해 접속하는 것입니다.
> - I2P 트래픽을 합법적인 방식으로 캡슐화하는 것입니다. VPN이 합법적이라면 VPN을 사용할 수 있고, SSH가 합법적이라면 SSH 터널을 사용할 수 있습니다.
>
> 하지만, 만약 당신의 적이 당신이 익명으로 다운로드하려는 특정 파일을 기다리고 있다고 가정해 봅시다. 만약 적이 당신이 HTTPS 터널이나 SSH 터널, 또는 VPN을 통해 비슷한 크기의 파일을 다운로드하는 것을 목격한다면, 그들은 그 파일이 당신이 익명으로 다운로드하려던 파일이라고 단정짓고 당신을 추적할 것입니다.
> 사실, 적이 모든 I2P 사용자, 모든 Tor 사용자, 모든 Bittorrent 사용자, TLS 사용자, 모든 Bitcoin 사용자 등을 표적으로 삼으려 한다면, 사람들이 절대 의심받지 않도록 보장하는 "설정"을 제공하는 것은 불가능합니다. 예를 들어, 여러분은 https://i2p.net/에서 실행 가능한 설치 프로그램을 다운로드했을 겁니다. 즉, "I2P에 관심이 있습니다"라는 DNS 요청을 보내고, I2P 웹사이트에 접속해서 약 18.5MB 크기의 파일을 다운로드했을 겁니다. 이렇게 엄격한 규제 체제에서는 비공식 채널, 아마도 Sneakernet 채널을 통해 I2P를 다운로드하거나, 아니면 이미 의심을 받는 상황에 놓이게 됩니다. 게다가 감시가 어려운 채널에서 시드 파일을 다시 제공해야 하는데, Sneakernet에서 제공한 파일이 처음부터 새것이기를 바라야겠죠. 인터넷 연결은 안테나 같은 걸로 합니다. 대충 어떤 상황인지 아시겠죠? 이처럼 억압적인 체제에서는 기술과 함께 탈출 계획을 포함한 철저한 준비가 필수적입니다.
> 다행히 현재까지 이러한 법을 제정한 나라는 극소수에 불과합니다.
>
> https://www.reddit.com/r/i2p/comments/bfh6cd/if_you_live_in_very_hostile_region_of_the_world/ @

> To me, the safest way to run freenet in a hostile country is the following:
>
> - Know Freenet users either in countries with more relaxed laws or people who know people
> - Install freenet in a VM that's using full disk encryption OR on a VPS in another country. If remote node, connect to fproxy via SSH tunnel. Deleting a VM using full disk encryption takes seconds and is hard to recover valuable data from.
> - Connect with friends as darknet peers. Make sure they're not an informant. This is an opsec thing.
> - Use Freenet

> Never run your node in anything but high security, even once.
> 제 생각에 적대적인 국가에서 Freenet을 안전하게 운영하는 가장 좋은 방법은 다음과 같습니다.
>
> - 법이 비교적 완화된 국가의 Freenet 사용자 또는 그들을 아는 사람들을 통해 Freenet 사용자를 확보하세요.
> - 전체 디스크 암호화를 사용하는 가상 머신(VM) 또는 다른 국가의 VPS에 Freenet을 설치하세요. 원격 노드인 경우 SSH 터널을 통해 fproxy에 연결하세요. 전체 디스크 암호화(Full Disk Encryption)를 사용하는 VM은 삭제하는 데 몇 초밖에 걸리지 않으며 중요한 데이터를 복구하기 어렵습니다.
> - 친구들과 Darknet 피어로 연결하세요. 정보원이 아닌지 반드시 확인하세요. 이는 작전 보안과 관련된 사항입니다.
> - Freenet을 사용하세요.
>
> 노드를 실행할 때는 절대로 최고 수준의 보안 설정 외에는 다른 설정을 사용하지 마십시오. 단 한 번이라도 사용해서는 안 됩니다.
>
> https://www.reddit.com/r/Freenet/comments/bfh6oe/if_you_live_in_very_hostile_region_of_the_world/ @

> If you're going to be in a place where you're worried about that, your laptop will be searched on arrival, and fairly well. You will need to go further, and hide the application. Maybe even compile it once you arrive.
> Being caught with these things on your computer upon entrance to said country might land you in prison.
> 만약 그런 문제가 걱정되는 곳에 가신다면, 도착 시 노트북 검사를 꽤 꼼꼼하게 받게 될 겁니다. 더 나아가, 해당 애플리케이션을 숨겨야 할 수도 있습니다. 어쩌면 도착 후에 직접 컴파일해야 할지도 모릅니다.
> 해당 국가 입국 시 컴퓨터에 이런 것들이 있는 것이 적발되면 투옥될 수도 있습니다.
>
> https://www.reddit.com/r/i2p/comments/bfh6cd/if_you_live_in_very_hostile_region_of_the_world/ @

https://www.whonix.org/wiki/Bridges

USER -(SSH)-> VPS -(Tor,I2P,Hyphanet,GNUnet)-> Website

신뢰할 수 있는 VPS에 Tor, I2P, Hyphanet, **GNUnet** 같은 프로그램을 설치하고 SSH로 터널링(Tunnelling)하여 ISP로부터 익명 네트워크 사용을 숨길 수 있다. ISP는 유저가 VPS와 SSH로 통신하고 있다는 사실만 알 수 있다. 단 이용하는 VPS를 신뢰해야 한다는 단점이 있다.

이 저작물은 CC BY-NC-SA 2.0 KR에 따라 이용할 수 있습니다. (단, 라이선스가 명시된 일부 문서 및 삽화 제외)
기여하신 문서의 저작권은 각 기여자에게 있으며, 각 기여자는 기여하신 부분의 저작권을 갖습니다.

나무위키는 백과사전이 아니며 검증되지 않았거나, 편향적이거나, 잘못된 서술이 있을 수 있습니다.
나무위키는 위키위키입니다. 여러분이 직접 문서를 고칠 수 있으며, 다른 사람의 의견을 원할 경우 직접 토론을 발제할 수 있습니다.